da
Sistemi&Impresa

n.7
Ottobre/Novembre/Dicembre 2023

PER INFO E ABBONAMENTI
www.este.it
Daniela Bobbiese | responsabile abbonamenti ESTE | 02.91434400 | daniela.bobbiese@este.it

La cybersecurity dopo le crisi geopolitiche Nuovi approcci per la sicurezza informatica

Le imprese hanno acquisito maggiore consapevolezza dei rischi. Ma mancano gli investimenti. E una cultura condivisa. L'obiettivo è oggi affrontare attacchi sempre più complessi ed evoluti

di Alessandro Gastaldi, con la collaborazione di Alessia Stucchi

Negli ultimi tre anni le crisi sanitarie, economiche e belliche susseguitesi nel panorama internazionale hanno cambiato drasticamente il volto della nostra società. Le imprese e le loro persone, per prime, hanno dovuto far fronte agli effetti diretti e indiretti di questi choc e nessuno ne è rimasto estraneo. A emergere in modo preponderante, tra gli altri, sono i rinnovati paradigmi legati alla cybersecurity: tra la remotizzazione del lavoro e la digitalizzazione delle imprese tipiche del periodo pandemico, i dati sono usciti dai tradizionali confini dell'azienda per essere immagazzinati, processati e analizzati in nuovi ambienti. Lo scoppio dei conflitti in Ucraina e in Medio Oriente ha accesso i riflettori su quelle che sono le implicazioni della guerra informatica su larga scala e di come sia meno complicato penetrare anche i sistemi di sicurezza degli organi governativi tecnologicamente più evoluti.
Al contempo, il numero di cyber attacchi rivolti alle imprese è drasticamente aumentato (40% nel primo semestre del 2023, come segnalato dall'Associazione italiana per la sicurezza informatica) e molte di queste – in particolare le Piccole e medie imprese (PMI) – devono fare i conti con la preparazione delle persone che, con i loro comportamenti e le loro attività possono compromettere la sicurezza informatica delle loro aziende. "Non bisogna chiedersi se ci sarà o meno un attacco, ma quando questo avverrà": il più comune aforisma del mondo della cybersecurity rispecchia oggi più che mai la realtà dei fatti; è quindi necessaria una riflessione sul nuovo contesto, sui rischi e sulle tecnologie utili a fronteggiarli.

Le persone al centro della sicurezza informatica

Nella visione della cybersecurity di Lenze Italia, divisione italiana della multinazionale tedesca specializzata in automazione industriale, i tre pilastri fondamentali sono tecnologia, processo e persone. "In questi anni abbiamo sventato numerosi incidenti grazie all'unione tra innovazione tecnologica, processi snelli e persone adeguatamente formate per interiorizzarli", commenta **Maria Civitano, Board Member e AFC Director di Lenze Italia**. Le soft skill giocano un ruolo fondamentale per implementare la strategia di sicurezza, a tal punto che,

Maria Civitano
Board Member e AFC Director di Lenze Italia

in Lenze, il personale investe il 20% del tempo di lavoro in attività di formazione per sviluppare le adeguate conoscenze tecniche. Grazie a corsi di aggiornamento svolti ogni sei mesi, i collaboratori imparano a riconoscere i tentativi di attacco informatico e le nuove tattiche utilizzate: "Il phishing è una tipologia d'attacco difficile da affrontare, perché arriva quotidianamente attraverso mail, sms e telefonate. I collaboratori devono fare proprie, innanzitutto, quelle semplici pratiche che però hanno un valore immenso per l'azienda", spiega Civitano. Per tutelarsi maggiormente è inoltre fondamentale utilizzare sistemi all'avanguardia per la condivisione di comunicazioni e documenti all'interno dell'organizzazione, dal momento in cui attraverso questi possono essere veicolati i vettori dell'attacco.
La filosofia di protezione informatica di Lenze Italia mette, quindi, le persone al centro, sottolineando l'importanza di attuare le corrette procedure in un contesto post pandemico dove gli scenari di attacco diventano sempre più sofisticati: "Prima del covid 19, la difficoltà principale risiedeva nel convincere i collaboratori al cambiamento, ma la pandemia ha costretto a prendere coscienza della digitalizzazione, delle opportunità e dei rischi a essa connessi. Le imprese devono essere lungimiranti e, per esserlo, devono conoscere le norme e le direttive della cybersecurity". Le diverse normative sono, infatti, un alleato di cui l'azienda deve dotarsi per rendersi conto dell'evoluzione dei criminali informatici. "In molti casi le organizzazioni pensa di essere dotata della migliore tecnologia, ma i sistemi di attacco si sono

Stefano Alei
South Europe Transformation Architect di Zscaler

sviluppati intensamente negli ultimi anni e per questo è fondamentale mantenersi aggiornati con gli strumenti di tutela adeguati", commenta la manager.
Relativamente al futuro della cybersecurity, che si appresta a includere tecnologie sempre più avanzate come l'Intelligenza Artificiale (AI), secondo Civitano il ruolo umano continuerà a giocare un ruolo determinante. "Il miglior controllore di qualità è colui che lavora, perché è l'esperto capace di elaborare le informazioni a disposizione. È l'uomo ad aver inventato la macchina, non viceversa, quindi sarà sempre lo specialista a gestire la sicurezza sfruttando le potenzialità degli strumenti, anche dell'AI".

La necessità di un cloud europeo

Negli ultimi tre anni, anche a causa delle ricorrenti crisi geopolitiche di cui si parlava in apertura, la cybersecurity è diventata una questione sempre più attuale e impellente, tanto da aver spinto le aziende a cercare riparo in una 'corsa alla tecnologia'. Come riportato dai dati segnalati da Zscaler, società attiva nel settore della cybersecurity, gli attacchi informatici tracciati sono raddoppiati, passando da 6.200 nel 2022 a 14mila nel 2023. "Uno dei motivi è lo scoppio della guerra in Ucraina, che ne ha scatenato una recrudescenza dopo che questi si erano intensificati durante il periodo pandemico, quando il numero medio di attacchi è arrivato a essere superiore di cinque volte rispetto al passato", commenta **Stefano Alei, South Europe Transformation Architect di Zscaler**.
L'attacco ransomware, come spiega il manager, consiste in un tentativo iniziale di accesso, per esempio attraverso le già illustrate campagne di phishing. Successivamente il software, muovendosi all'interno dell'organizzazione, comunica ai criminali informatici le informazioni di maggior valore. "Gli attacchi ransomware sono sempre ben progettati e molto efficaci poiché silenziosi. Gli agenti malevoli, infatti, possono essere presenti per diversi mesi all'interno della Rete aziendale prima di rivelarsi con un'azione concreta", commenta Alei. Le infrastrutture tecnologiche, attraverso la migrazione dei gestionali e dei core business in cloud, si stanno espandendo e secondo Alei è necessaria una riflessione più ampia: "In Europa si è aperto il dibattitto relativo alla *sovereignty cloud*, cioè la sovranità dei nostri dati. I principali strumenti commerciali sono statunitensi e questo mette le aziende e la Pubblica amministrazione in difficoltà quando si tratta di avere controllo totale delle informazioni. Si sta lavorando nella direzione di cloud europeo, ma si tratta di una sfida enorme poiché questo deve contemplare le esigenze di 27 Paesi".
Nel frattempo, il mercato si sta uniformando su una serie di tecniche e approcci, come lo zero trust. Si tratta di un paradigma mirato a garantire l'accesso alle risorse assumendo di essere già in un contesto minacciato: la richiesta di accesso a una determinata informazione non avviene quindi direttamente, ma è mediata da un'analisi protettiva che permette di rilevare l'identità di chi vuole

accedere: "Questo approccio si traduce nella creazione di sessioni 'blindate' prima e dopo il superamento dell'analisi. In questa comunicazione mediata l'aspetto più importante è la Ssl Inspection, cioè l'apertura di codici cifrati. Questo passaggio è fondamentale perché il 90% degli attacchi informatici avviene tramite la cifratura delle comunicazioni", conclude Alei.

La protezione delle aziende passa dalla lungimiranza

Per meglio comprendere la sensibilità delle imprese italiane in merito alla cybersecurity, Certego, società di VEM Sistemi specializzata in servizi di sicurezza IT, ha commissionato a Ipsos, azienda che si occupa di analisi di mercato, il report di ricerca Cybersecurity 2023: qual è la consapevolezza delle aziende italiane?, svolto su un campione di 220 imprese pubbliche e private per analizzare la sensibilità e preparazione delle aziende italiane in merito ai temi della cybersecurity e della digitalizzazione . "Attraverso i nostri sensori raccogliamo i dati dei clienti, che sono principalmente medie e grandi aziende. Grazie alla partnership possiamo, così, estendere l'analisi alle PMI", commenta **Alessandro Di Carlo, Forensics & Product Manager di Certego**. Uno degli output emersi è l'aumentata bravura capacità delle aziende di consulenza cyber, ma anche direttamente delle piccole e medie imprese PMI nel riconoscere un attacco informatico.

Le matrici degli attacchi sono evolute nel tempo, partendo dagli albori di internet dove lo scopo principale era dimostrare la forza degli attaccanti, per esempio quando un sito web era compromesso, per arrivare a oggi dove l'obiettivo è un ritorno economico. "Chi ricorre all'uso

Alessandro Di Carlo
Forensics & Product Manager
di Certego

di ransomware è strutturato in vere e proprie aziende. Il loro obiettivo è monetizzare rendendo indisponibile il know how aziendale mediante cifratura, totale o parziale, dell'infrastruttura", commenta Di Carlo. Quest'area degli attacchi informatici ha aiutato a promuovere la sensibilità delle imprese, perché, se una decina di anni fa circa il 95% delle aziende vedeva la cybersecurity come un costo, oggi il dato è notevolmente migliorato, anche se, come emerge dall'analisi con Ipsos, quasi il 35% delle PMI ancora non la considera un valido investimento.

A causa delle ricorrenti crisi geopolitiche, oltre all'attacco per soli obiettivi economici, è inoltre rilevante la macro area di spionaggio: "Rispetto a un attacco ransomware, in caso di spionaggio l'attacco è più subdolo, perché fatto su misura; l'attaccante punta a compromettere Reti aziendali cercando di lasciare meno tracce possibili e limitando al minimo il suo 'rumore', e per farlo ha bisogno di un periodo di tempo abbastanza lungo che gli consenta di studiare il suo obiettivo con estrema attenzione", commenta il manager. Esistono anche situazioni dove le due dimensioni si intersecano e, in questi casi, è necessaria un'organizzazione complessa: "Il gruppo Conti, un'organizzazione criminale noto anche per aver apertamente appoggiato la compagine russa durante la guerra in Ucraina, per esempio, è strutturato come una vera e propria azienda, i suoi affiliati lavorano otto ore e sono addirittura supportati da una struttura HR".

In seguito allo scoppio del conflitto e all'emergenza pandemica, quindi, si è consolidato nel panorama attuale un maggiore tasso di investimento nella cybersecurity, ma con un limite: "L'80% delle imprese si sente sicura nell'adottare solo tecnologie preventive, ma se la prevenzione fallisce e non sono presenti tecnologie di rilevamento, per l'analista è molto difficile comprendere cosa staia esattamente succedendo", commenta Di Carlo. Per il futuro, a suo giudizio, l'azienda deve essere più resiliente e lungimirante al fine di avere la giusta visibilità all'interno della propria infrastruttura informatica.

Diffondere una cultura della sicurezza

L'infrastruttura informatica è considerata un aspetto sempre più strategico della filiera produttiva, per questo le aziende (incluse le PMI) secondo Bitia, società sviluppatrice di soluzioni per la digitalizzazione, si stanno

attrezzando per essere più resilienti per affrontare un eventuale cyber attacco. "La richiesta principale che riceviamo dalle aziende è il pressure test, cioè l'analisi delle debolezze del sistema. Le imprese vogliono conoscere la loro capacità di affrontare un attacco, arrivi dall'esterno o dall'interno", commenta **Simone Bittarello, CTO & Security Manager di Bitia**.
Su questo fronte, la principale sfida da cui le aziende devono tutelarsi è il phishing, in quanto si tratta ancora della minaccia più diffusa: "Queste tecniche sono sempre più sofisticate e le mail utilizzate sempre più credibili, quindi è facile cadere nel 'tranello' criminale". Negli ultimi anni, inoltre, stanno diventando sempre più frequenti i tentativi compiuti attraverso le falle di sicurezza delle applicazioni aziendali come, per esempio, i portali gestionali. Per questo motivo si sta affermando il processo di code review, cioè l'analisi del codice sorgente delle applicazioni implementate. "Il code review Sta diventando uno standard all'interno delle imprese, perché la sicurezza non nasce solo dagli aspetti infrastrutturali, ma dall'applicazione stessa che deve essere monitorata nelle varie versioni", commenta il manager.
A dover essere analizzata, oltre all'applicazione aziendale, è anche l'IoT, in particolar modo l'interconnessione dei macchinari, in quanto i nodi delle Reti aziendali possono costituire un punto d'accesso dell'attacco informatico: "Un'infrastruttura di Rete corretta prevede che i macchinari e i sistemi siano segregati, non ci deve essere rischio di entrata da ciò che è esterno all'azienda", spiega il manager. Gli antivirus tradizionali non sono quindi più sufficienti a proteggere l'azienda e l'elemento su cui gli specialisti stanno puntando sono i next generation antivirus, che sfruttano l'AI e altri meccanismi di controllo.
Per il futuro, secondo Bitia, così come è stato il percorso verso il cloud che si è affermato in modo preponderante tra le aziende negli ultimi anni, anche la cybersecurity compirà lo stesso sviluppo: "Le tecniche e gli strumenti di attacco sono oggi alla portata di tutti, perché chiunque può dotarsi di uno strumento idoneo alla causa, quindi per le aziende è fondamentale tutelarsi in modo opportuno. La parola chiave, oggi, dovrebbe essere 'cybersecurity first', proprio perché serve diffondere una cultura della sicurezza", conclude Bittarello.

Il maggiore pericolo è l'inconsapevolezza

Prima della pandemia, molte aziende non comprendevano la necessità di investire per difendersi dagli attacchi informatici, soprattutto se fino a quel momento non ne avevano subiti. La pandemia, però, ha modificato la percezione delle imprese perché, con un aumento degli accessi da remoto, i sistemi informativi sono stati maggiormente interessati da un aumento dei rischi legati alla cybersecurity. Secondo Bitdefend Italia, società informatica specializzata nella programmazione di software per la sicurezza, quello del lockdown si è rivelato un periodo particolarmente proficuo per gli hacker: "In quel contesto, gli attaccanti sono riusciti a recuperare importanti moli di dati sensibili, evidenziando una diffusa mancanza di sicurezza nelle reti aziendali", commenta **Fulvio Fabi, National Channel Manager di Bitdefender Italia**.
A oggi, però, ancora molte aziende ritengono che non valga la pena destinare risorse consistenti per tutelarsi dai cyber attacchi: "Il problema principale è che nessun operatore, per nessuna cifra, è in grado di assicurare la protezione totale e questo spaventa le imprese", commenta Fabi. Lo scenario che emerge è caratterizzato, infatti, da una continua evoluzione, perché così come gli specialisti della cybersecurity lavorano costantemente per proteggere le aziende, allo stesso tempo gli hacker operano per aggirare queste protezioni. Secondo il manager, inoltre, la diffusione dell'IoT, e la conseguente interconnessione dei macchinari in azienda, aumenta la superficie d'attacco: "Anche una macchinetta del caffè con entrata Usb oppure una stampante wireless sono porte di accesso ai dati aziendali e, per questo, sono potenzialmente attaccabili".
La strategia primaria per tutelarsi è, quindi, la formazione interna, cioè condividere le conoscenze basiche del reparto IT al restante personale in azienda. "Se il budget a disposizione dell'azienda è limitato, bisogna partire dalla formazione, perché il pericolo principale all'interno delle organizzazioni è il lavoratore poco informato", commenta il manager di Bitdefender Italia. La società, inoltre, trasmette nozioni di base alle aziende con cui collabora, come la tipologia di password da impostare, quali siti evitare sui dispositivi aziendali e le principali tecniche di protezione dal phishing. La sensibilizzazione dei collaboratori a queste tematiche è, senza dubbio, il primo passo per tutelare i dati aziendali.

Simone Bittarello
CTO & Security Manager
di Bitia

Fulvio Fabi
National Channel Manager
di Bitdefender Italia

La cybersecurity è anche questione di reputazione

Per tutelarsi dagli attacchi informatici, le aziende dovrebbero attivare una serie di processi che permettano di segregare le Reti industriali, mitigare i rischi e identificare le possibili vulnerabilità. Questa attenzione deve essere presente non solo all'interno dell'azienda stessa, ma in tutta la Supply chain in quanto, come sottolinea Hermes Reply, società di consulenza e system integration, la manutenzione remota a cui le imprese si affidano per la diagnosi degli impianti, delle linee di produzione e dei robot, può costituire una sorta di porta per accedere all'interno delle organizzazioni. "Il manutentore, a volte, è più vulnerabile, rispetto all'azienda per cui svolge il servizio e, per questo motivo, più facilmente attaccabile da un hacker che, attraverso lui, penetra all'interno della Rete aziendale", commenta **Massimiliano Oddi, CEO di Hermes Reply**.

Gli attacchi informatici, indipendentemente dal punto di accesso, generano diverse tipologie di conseguenze per le aziende che li subiscono. Innanzitutto il danno reputazionale (in particolar modo se l'impresa è pubblica e quotata), poiché si deve dar riscontro al mercato di essere stati attaccati. Un'altra problematica è il danno legale che si produce quando sono state rubate informazioni sensibili, come brevetti o dati di proprietà intellettuale, in quanto gli investitori possono rivalersi sul danneggiamento delle loro quote di valore. "Il danno legale si traduce immediatamente in un danneggiamento economico, che può essere diretto, in caso di blocco della produzione, oppure indiretto, in caso di richiesta di riscatto delle informazioni sensibili", spiega Oddi.

Massimiliano Oddi
CEO
di Hermes Reply

Diego Marson
Chief Technology Officer
di Yarix

Negli ultimi due anni, in termini di sensibilizzazione, il CEO di Hermes Reply ha notato una maggiore consapevolezza delle PMI nell'impostare un più efficiente modello tecnologico: "Oggi il 70 % delle aziende che vogliono mitigare il rischio cyber si affidano a strumenti di controllo e di mitigazione del rischio che, dal punto di vista software, utilizzano algoritmi di AI e di Machine learning, mentre la parte restante delle aziende mantiene strutture di protezione classiche". Un'ulteriore tendenza messa in luce dall'esperto è il trasferimento del business su piattaforme cloud, così da ottenere un maggiore vantaggio competitivo e, allo stesso tempo, esternalizzare i rischi della tutela informatica. "Molte imprese, trasferendo i loro dati in cloud, demandano la responsabilità della loro sicurezza al fornitore esterno. In caso di attacchi, la responsabilità demandata è anche assicurativa, perché sono i fornitori a dover rispondere formalmente a eventuali falle", conclude Oddi.

Sotto copertura nel dark web

Gli attacchi più temuti oggigiorno dalle aziende implicano il furto di dati sensibili, la cifratura per impedirne l'accesso e una successiva richiesta di riscatto. Nel contesto italiano, secondo Yarix società a capo della Business unit Digital Security di Var Group, i principali vettori di accesso sono due: da una parte i sistemi esposti con autenticazione debole o non aggiornati, specialmente nel caso di accesso da remoto (come le vpn) non adeguatamente protetto, dall'altra le Reti raggiungibili pubblicamente e prive delle necessarie tutele. **Diego Marson, Chief Technology Officer di Yarix**, spiega infatti come la mancanza di autenticazione *multi factor* grazie a un secondo riconoscimento sia oggi una mancanza fondamentale: "Se il criminale riesce a sottrarre le credenziali di un utente può accedere alla rete aziendale. Per questo motivo è fondamentale monitorare il dark web o i forum underground per sapere se queste informazioni sono state intercettate".

È quindi di rilevante importanza intervenire nel darkweb per recuperare le credenziali sottratte prima che queste siano acquistate da altri. Per agire in tempo, il team di Yarix si avvale di bot che analizzano i pattern di infiltrazione -così da poterli riconoscerli in seguito- e sull'attività specifica e manuale di un team che lavora sotto copertura. "L'accesso ai forum e il successivo acquisto dei dati dipende dalla reputazione dell'acquirente. Gli attaccanti devono fidarsi di chi si interfaccia con loro, è quindi necessario che il team di 'infiltrati' abbia un'elevata referenzialità" commenta Marson. Tra le varie strategie adottate, lo specialista sotto copertura riesce a guadagnare un giudizio positivo quando conclude transazioni 'civetta', ovvero l'acquisto di dati poco interessanti (magari già pubblici), ma necessari a ottenere la fiducia del cyber criminale.

In futuro, il lavoro dello specialista sarà impattato dalle nuove tecnologie. Tra queste, l'AI generativa che può essere alimentata con casi di successi e, dopo l'allenamento, poter rispondere agli input somministrati con maggiore esperienza. Secondo Marson, però, il

fattore umano rimarrà determinante. "L'AI potrà arrivare a coprire un'ampia quota delle attività dell'esperto di cybersecurity, ma rimarrà comunque necessaria la competenza umana su temi specifici. Nei prossimi tre anni credo che potremmo assistere a uno scenario dove l'80% degli attacchi effettuato con l'AI si confronterà con l'80% degli interventi difensivi basati sulla stessa tecnologia. Sarà interessante comprendere, quindi, cosa avverrà sul restante 20%, quello dei due fronti basati sull'apporto umano", conclude il Chief Technology Officer di Yarix.

Identità sicure grazie al Privileged access management

Tutelare le credenziali di accesso degli amministratori aziendali significa proteggere l'intera impresa da eventuali attacchi informatici, questa è l'idea alla base del Privileged access management (Pam). Attorno a questa strategia – considerata pioneristica fino a pochi anni fa, ma oggi più diffusa – è nata Cyberark, azienda specializzata nei sistemi di sicurezza delle identità informatiche in azienda. "Fino a circa tre anni fa, Pam era un concetto di nicchia, perché dedicato ai soli ruoli apicali. In seguito alla pandemia, quando molteplici figure operative dovevano accedere da remoto alle Reti aziendale, è esplosa la necessità di proteggere i collegamenti dell'intero ecosistema aziendale", commenta **Paolo Lossa, Country Sales Director di CyberArk**.

Indipendentemente dalla posizione gerarchica ricoperta all'interno di un'organizzazione, qualsiasi utente – in base all'azione che deve svolgere – può essere considerato privilegiato, come spiega il manager: "Lo è, per esempio, il Direttore del Personale che deve interagire con un'applicazione contenente i dati personali di tutti i collaboratori. In quel contesto specifico, infatti, ha la necessità di accedere a informazioni sensibili e, di conseguenza, sono necessarie forme di controllo più serrato. La sicurezza delle identità umane e delle macchine deve, quindi, attraversare in modo trasversale tutta l'azienda".

La necessità di tutela generalizzata delle organizzazioni è fondamentale perché, come sottolinea Lossa, i principali scenari di attacchi di successo si basano tutt'ora su una compromissione di credenziali. Per questo motivo, la nuova sfida riguarda la gestione dell'accesso sicuro al cloud e al multicloud, ovvero la condizione di pluralità dei servizi di Cloud computing fruiti da un'azienda: "In questi casi, le aziende possiedono diverse piattaforme dedicate ai loro sistemi e la loro sicurezza può essere tutelata solo attraverso tool di governance centralizzati". Per proteggere i dati sensibili l'azienda deve, secondo il manager, selezionare il giusto fornitore di servizi, automatizzare i processi per orchestrare le diverse componenti e, infine, dotarsi di strumenti che consentono un monitoraggio continuativo dei processi.

Nel panorama aziendale italiano, pur essendosi diffuso un maggior livello di consapevolezza, permane un gap tra la volontà di investimento delle aziende e l'effettiva

Paolo Lossa
Country Sales Director
di CyberArk

Massimiliano Dal Cero
Fondatore
di Digital Defense

disponibilità di persone con la giusta esperienza per gestire i progetti. "Questa mancanza di personale competente è un freno al potenziale di crescita dell'Italia in questo ambito. L'attenzione alla cybersecurity deve, invece, diventare la mission critica del Paese nella sua totalità e può essere efficacemente sviluppata solo attraverso la formazione", conclude Lossa.

La cybersecurity è un processo, non un prodotto

In Italia c'è una maggiore consapevolezza dell'importanza della protezione informatica ma, allo stesso tempo, non sempre emerge una reale volontà di investire. Soprattutto per quanto riguarda le PMI, secondo Horsa, realtà ICT italiana di progettazione e implementazione tecnologica, la spinta a investire sulla tutela informatica ha difficoltà a svilupparsi perché non esiste una vera sensibilità trasversale nell'organizzazione. "La sicurezza non è un prodotto, ma un processo, quindi coinvolge, oltre alla tecnologia, includono il fattore umano. Molte imprese faticano ad applicare il concetto, perché si limitano a cercare una protezione tecnologica, senza investire sulla formazione interna", spiega **Massimiliano Dal Cero, Fondatore di Digital Defense**, società del gruppo Horsa specializzata in cybersecurity.

Per abbracciare il corretto processo serve, secondo il manager, un cambio di paradigma: la cybersecurity non è solo applicazione tecnologica, ma un problema multidisciplinare che coinvolge l'ambito normativo. "Le aziende devono rispettare le norme del settore dell'azienda, quelle europee e quelle nazionali. Eppure, oggi molti tecnici peccano nella volontà di contemplare le ripercussioni normative del loro lavoro", commenta Dal Cero. Lì dove le competenze non solo presenti all'interno

Alessio Aceti
CEO
di HWG Sababa

dell'aziende, è necessario rivolgersi a consulenti esterni che sappiano consigliare le imprese su questo fronte.
Strutturare un nuovo approccio alla protezione informatica significa anche studiare in anticipo le procedure da attivare in caso di incidente per poter gestire lo stress, orchestrare le figure operative e preservare la prova digitale. Dal Cero sottolinea come la preservazione della prova digitale, a fini di denuncia e di analisi interne, sia fondamentale: "Il dato digitale è effimero e se non è attiva una procedura di preservazione, svanisce rapidamente e non si può recuperare. Attrezzarsi in anticipo è essenziale per imparare dagli incidenti e non esserne solo una vittima".
In questi anni l'evoluzione di approccio alla cybersecurity è avvenuto anche da parte di chi tenta di entrare nelle Reti aziendali: "Gli attacchi sono sempre più strutturati in una filiera con all'interno diverse specializzazioni, una vera e propria organizzazione, per cui non esiste più la figura romanzata dell'hacker che agisce da solo. La sfida delle imprese è, quindi, quella di attivare sistemi di protezione per poter affrontare la complessità evolutiva del lavoro, degli attaccanti e del contesto geopolitico", conclude Dal Cero.

Tecnologie affidabili per imprese più mature

La consapevolezza riguardo alla cybersecurity varia a seconda del settore, della dimensione e della maturità dell'azienda. Tuttavia, secondo HWG Sababa, provider di cybersecurity nato nel 2023 dalla fusione delle due omonime società, è possibile definire tre macro tipologie di aziende: le imprese virtuose, cioè quelle che hanno strutturato modelli di protezione cyber in maniera preventiva; le aziende che solo adesso stanno percependo i rischi; le organizzazioni che ancora non si sono mosse per affrontare la questione. "Tra le virtuose ci sono le società nei settori più critici, come banche, assicurazioni e multiutility. Si tratta di aziende che hanno nel loro Dna un'attenzione particolare ai temi della sicurezza", approfondisce **Alessio Aceti, CEO di HWG Sababa**. Il tessuto imprenditoriale italiano, ricco di imprese medio-piccole, rientra però solo marginalmente nella prima tipologia, e fa fatica a comprendere le reali necessità. l'importanza di proteggersi dagli attacchi cyber.
Complice di questa situazione, secondo il manager, è la varietà del panorama degli esperti, che si suddividono tra gli specialisti verticali e le società di consulenza IT che, tra i vari servizi, si occupano anche di sicurezza informatica: "Sul mercato troviamo molti strumenti inadatti, soluzioni che non garantiscono neanche il livello minimo di sicurezza informatica. Se il cliente di grandi dimensioni riesce a comprendere la differenza di qualità e efficacia dei prodotti, per le PMI è più complesso". La necessità di tutelarsi è, però, un'urgenza sempre più impellente, perché il contesto geopolitico innesca un circolo vizioso: i Governi aumentano gli investimenti in nuove tecniche di spionaggio e attacco, spesso riciclate dalla criminalità informatica internazionale al fine di penetrare nelle Reti delle imprese – con strategie sempre più innovative – proprio per scopi economici.
La strategia di HWG Sababa per affrontare le minacce attuali e future si basa, innanzitutto, sulla protezione di tutta la superficie di attacco, inclusi i dispositivi IoT, i sistemi di controllo industriale e i macchinari interconnessi, oltre all'integrazione dell'AI nei sevizi di security operation: "Gli specialisti devono migliorare la detection e altri aspetti tecnici, integrando sempre di più logiche di Machine learning nella gestione delle anomalie riscontrate sui sistemi dei clienti". Infine, deve aumentare la consapevolezza dell'intera organizzazione a proposito delle possibili modalità di attacco, che diventano sempre più realistiche e, quindi, difficili da indentificare.
Indipendentemente dalla qualità della tecnologia e della soluzione, secondo Aceti, gli elementi fondanti di una efficace strategia di protezione devono riguardare governance, processi e procedure, perché se un'azienda non ha chiara la gestione quotidiana della sua organizzazione, non può rilevarne le anomalie in caso di attacco: "La maggior parte delle crisi si verifica a causa di 'leggerezze' durante le procedure. Bisogna invece imparare a non fidarsi e a verificare continuamente".

ESTE
Cultura d'impresa

NON C'È **SVILUPPO** SENZA **CULTURA D'IMPRESA**

I prodotti editoriali ESTE sono da oltre sessant'anni un punto di riferimento per l'aggiornamento professionale di manager e imprenditori

Sviluppo & Organizzazione
Persone & Conoscenze — La voce della Direzione del Personale
SISTEMI&IMPRESA — Management e tecnologie per le imprese del futuro
MIT Sloan Management Review Italia
I,WE — INCLUSION, WELFARE, ENVIRONMENT

ABBONATI ORA

Le riviste ESTE sono distribuite solo su abbonamento. Abbonati sul sito www.este.it alla **versione cartacea+digitale** oppure scopri i pacchetti **abbonamento digitali** scaricando l'**APP ESTE.**

Per informazioni:
Daniela Bobbiese – Responsabile Abbonamenti ESTE
02.91434400 – daniela.bobbiese@este.it

GET IT ON Google Play
Download on the App Store